

REMARKS/ARGUMENTS

1.) Claim Amendments

The Applicant has amended claims 1, 3, 10, 13, 19, 25 and 31. Accordingly, claims 1-32 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

2.) Claim Rejections – 35 U.S.C. § 102(b)

The Examiner rejected claims 1-8, 10-17, 19-22, 24-28 and 30-32 under 35 U.S.C. § 102(b) as being anticipated by Jablon (US 6,226,383). The Applicant has amended claims 1, 3, 10, 13, 19, 25 and 31 to better distinguish the claimed invention from Jablon. As amended in claims 1, 3, 10, 13, 19, 25 and 31, the present invention is clearly distinguishable over Jablon. As amended, the present application discloses authenticating the first and second contributions using a *message authentication code* and *passcode*. In contrast, Jablon discloses a completely different approach. Jablon does not explicitly authenticate the contribution values but instead, at a later step, verifies the shared secret, resulting from the Diffie-Hellman key exchange.

Regarding claim 2, whereas user interaction alone is not novel (nor is it for any other password based key exchange), user interaction, in combination with the other novel features of claim 1, it is patentably distinct from Jablon.

Regarding claim 3, Applicant respectfully traverses the Examiner's interpretation of Jablon. The Examiner states that Jablon teaches a method (col. 6 line 66 to col. 7 line 31) where the passcode is encrypted by the second unit using the shared secret and transmits the encrypted passcode to the first communication unit together with the generated second contribution. However, this is not disclosed by Jablon in any of the described protocol interactions. Rather, Jablon discloses a method where a long-lived Diffie-Hellman integer exponent based on the password is used in the key-exchange — this is significantly different from the protocol of the present application.

Regarding claim 4, while Jablon discloses a key exchange method based on the Diffie-Hellman key exchange, the method of the present invention operates differently as discussed with regard to claim 1.

Regarding claim 5, Jablon discloses that the password (or passcode) is given to both parties in the key exchange, but Jablon does not disclose a protocol interaction where the passcode is *generated* in the first device and then given to the second device using user interaction. The foregoing is not at all discussed in col. 6, or 7 or any other part of Jablon.

Regarding claim 6, Jablon, in col. 22, lines 23-34, discusses use of a MAC to authenticate the shared secret (K) that is the result of the SPEKE key exchange. This is different from claim 6 of the present invention wherein it *authenticates* the first and second contributions (i.e. not the shared secret that is the result of the key exchange) using a MAC and the passcode. In particular, Jablon does not discuss any method that uses the shared passcode to calculate the MAC.

Regarding claim 7, the use of an error-correcting code is not disclosed in col. 6, 7 or 22 of Jablon, or any other part of Jablon, for that matter.

Regarding claim 8, Jablon discusses at col. 15, line 10 a one-way mapping function to be used in accordance with that invention. This mapping function uses one-way properties and suggests using exponentiation and a suitable group. However, there is no connection between an error-correcting code function of the present invention the one-way function of Jablon.

Regarding claim 10, the Examiner states that the present invention is disclosed by Jablon. However, as noted with respect to claim 1, such is not the case. In claim 10, the *first* contribution is authenticated before the second contribution is sent. Jablon does not suggest that any authentication or verification takes place until the secret key has been agreed between the two parties (see the Figures of Jablon).

Regarding claims 11 and 12, the claimed procedures of the present invention are not disclosed by Jablon as Jablon discloses a completely different protocol and approach.

The comments with respect to claims 1, 5-8 are applicable to claims 13-17 respectively; the comments with respect to claims 1, 7-8 are applicable to claims 19-22

respectively; the comments with respect to claim 3 are applicable to claims 24 and 30; the comments with respect to claims 1, 6-8 are applicable to claims 25-28 respectively and the comments with respect to claim 1 are applicable to claims 30-32.

3.) Claim Rejections – 35 U.S.C. § 103(a)

The Examiner rejected claims 9, 18, 23 and 29 under 35 U.S.C. § 103(a) as being unpatentable over Jablon. The Applicant has amended claims 1, 13, 18 and 25, from which claims 9, 18, 23 and 29 indirectly depend to better distinguish the claimed invention from Jablon. The Examiner's consideration of the amended claims is respectfully requested.

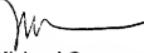
CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

Date: 3/22/01


Michael Cameron
Registration No. 50,298

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-4145
michael.cameron@ericsson.com